The Challenges and Countermeasures of Blockchain Finance and Economics

Yang Zheng[#1], Tao Huang[*2]

[#] *School of Business, University College Dublin & School of Economics and Management, Xidian University, Belfield, Dublin 4, Ireland*

[*]*School of Microelectronics, Xidian University, 266 Xinglong Section of Xifeng Road, Xi'an, China*

[1]yang.zheng@ucdconnect.ie

[2]htao156@163.com

Abstract **- Blockchain is a new underlying technology in the Internet era, whose ultimate goal is to analyse and process the information data through the effective integration of financial resources. No matter what kind of financial formats or new financial service models are generated, they are all dedicated to upgrade the financial system and promote the efficiency and quality of financial operations and service from the layer of data, rules, and application according to the market and customer needs. Blockchain technology can help the financial industry to automatically and accurately identify customer credit conditions to restructure the financial market credit system and improve the efficiency of cross-border payment. However, it also poses a challenge for the development of the financial industries. In this paper, we systematically analyse the technology of blockchain and its application in the financial and economic field, the status quo and the challenges it faces, and then give constructive suggestions to help the blockchain technology develop better in the financial and economic field.**

Keywords *- Blockchain; finance and economics; challenges; countermeasures.*

1. Introduction

Blockchain (distributed ledger technology) is a network software protocol that enables the secure transfer of money, assets, and information via the Internet, without the need for a third-party intermediary such as a bank (Swan, 2015). It can safely store transactions, such as digital crypto-currencies, or other data such as information about debt, copyrights, equity and digital assets in general, the stored information cannot be easily forged and tampered with, as that would involve individual approval of all distributed nodes. This greatly reduces the cost of trusting and accounting that are commonly found in non-digital economies and other non-digital social activities. Blockchain is mainly comprised of a:

- hash, which maps, using one-way mathematical functions to assign unique indexes;
- digital signature, which is implemented as a public cryptographic key;
- P2P network, which serves as a routing structure for nodes to use the distributed hash;
- consensus mechanism, which is a set of digital procedures designed to ensure the accuracy and consistency of the stored information across the participating nodes.

Each block is composed by a head and a body, packaging its version number, the address of the previous block, the current block's target function, work proof and other consensus data such as timestamp and Merkle root, whose data structure is shown in Figure 1. The latter is a part of Merkle Hash Tree (which is a tree that can be either a binary tree or a multi-tree in the data structure, information data is recorded as the hash value stored in Blockchain body, the generated Merkle root through Merkle tree's hash process will be recorded in blockhead).

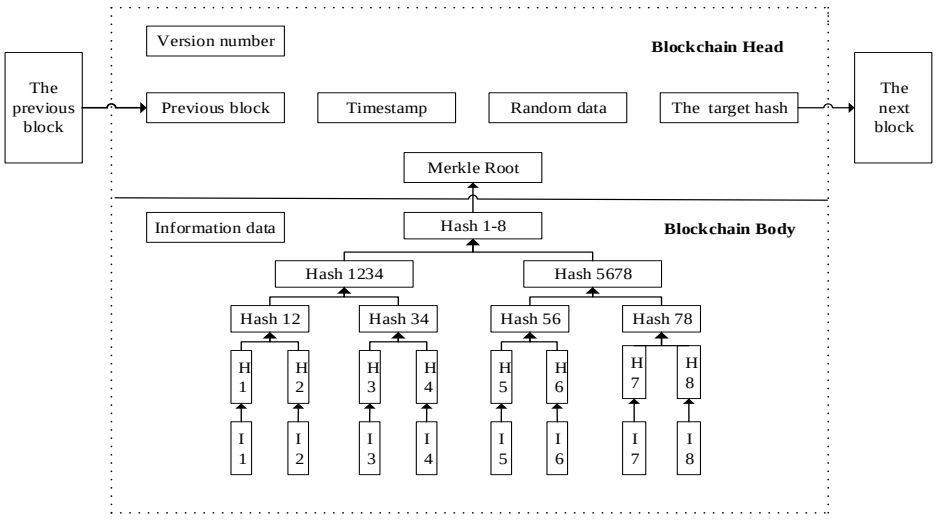

Figure 1. The Blockchain Data Structure

The Blockchain technological platform is gradually shaping up into the following directions:

- underlying infrastructure, which includes facilities for mining and manufacturing of specialized computer hardware to perform blockchain-related tasks;
- middle layer between the Blockchain platform and client application services, including smart contracts, Blockchain platform, financial software and other services;
- hotspot distributed applications in various industries, including Finance (such as cross-border payments, liquidation, financial services, and asset digitization), Cyber Security (such as identity protection, data authenticity protection, and critical infrastructure protection) and Supply Chain (such as logistics tracking and Digital works achieving process tracking).

It is reported that the private data of an estimated 145.5 million Americans were exposed by the Equifax credit attack (Cowley, 2017) and, in another major attack, the names, emails, and passwords of all 3 billion Yahoo user accounts were stolen, (Khandelwal, n.d.) so greater user control and permissioning of personal data is expected by most people. Cybersecurity could be one of the biggest drivers of blockchain adoption for the blockchain technology is called "trustless" in that they confirm and transfer value directly without having to trust any third party institution in the middle of transactions with personal data. The result is a trustless system in that the human counterparties and institutions involved do not need to be known and trusted. Instead, trust is placed in the computational smart network system, which could help to create next-generation cybersecurity solutions.

It has been confirmed that the investment in Blockchain is concentrated in western developed countries, while the United States occupies the leading position in investment in the Blockchain. Most major European countries are open to Blockchain technology. Australia, Canada, Toronto, and South Korea plan to upgrade their systems through Blockchain technology, Russia holds a moderate attitude toward Blockchain technology and Israel becomes a Blockchain innovation center (Zhou, Li, & Guo, 2017, pp. 37–38). At present, Blockchain has attracted many enterprises to invest in it because of open source. The types of projects include data security, cross-border payment, settlement of financial market transactions, trade finance, cybersecurity, insurance, real-time money transfer, property registries, contractual agreements, and identity confirmation, smart contracts and auctions, attack detection and so on. The finance and economic field are the most widely used sections of blockchain application.

2. The application of blockchain in finance and economics

2.1 Blockchain economic and financial theory cornerstone

There are three main theories relevant to this application, the first one is Digital Economy Theory, whose facts and introductions are analyzed by authors (Illing & Peitz, 2005) in detail. Blockchain economics and finance promote the convergence of computer and communications technologies, digitize all assets and register and transfer notarized on the

blockchain, aiming at realizing the complete digitization of goods and services from manufacturing, sales, and supply chain. The second theory is Free Currency, the author (Chen, 2017) elaborated the dialectical relationship between money and freedom from the perspective of Marx's economic philosophy deeming that the monetary system should not be issued by one government and the central bank but should be completely decentralized and non-state-owned. All kinds of digital currencies can be exchanged freely and without cost in the blockchain economy, the digital currency repeats the emergence, elimination, and evolution of the competitive process at an extremely rapid rate at present. The third one is Information Asymmetry Theory studied by three American economists (Cristian, Tudor, & Bolos, 2010), putting forward that the trust problem will arise as the information held by both parties is different. This theory provides methodological guidance for blockchain finance and economics since blockchain can realize the optimal allocation of resources through the form of digital rewards for mining aiming at establishing decentralized credit for universal participation.

2.2 The overall structure of blockchain finance and economics

As a new underlying technology in the Internet age, no matter what kind of financial and economic format is combined with the development of new business models, the ultimate goal of the blockchain is to use new Internet technologies such as big data and cloud computing to effectively integrate financial information resources, whose purpose is to promote the operation efficiency and service quality of the financial system by analysing the information data and upgrading the financial system according to the markets and customers' need. The overall structure of blockchain finance and economics is divided into three layers shown in Figure 2.

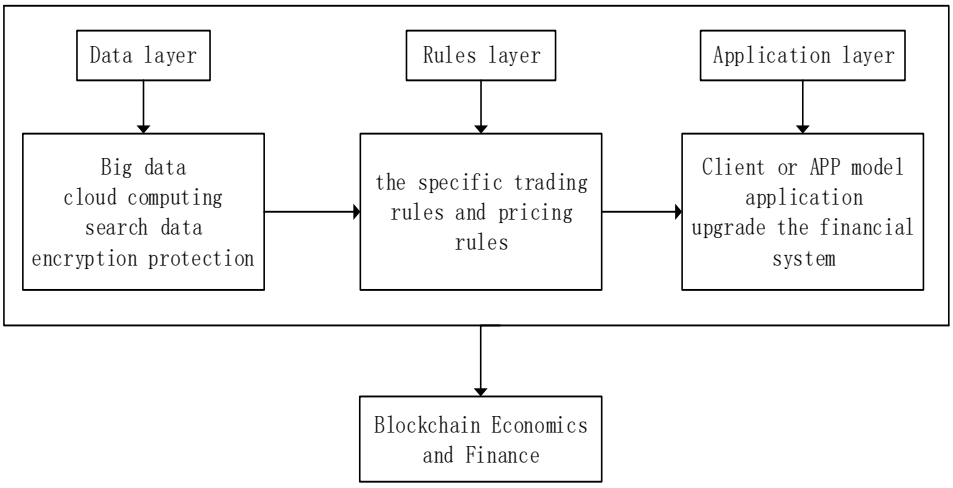

Figure 2. The overall framework of economy and finance in blockchain

Each layer has its own unique characteristics, data collection and analysis can be addressed through big data and cloud computing technologies at the blockchain financial data layer. While the security problem of blockchain data can be solved effectively when using the encryption algorithm. In the rule layer, a variety of traditional finance can be transformed into a new financial format based on blockchain's two basic rules of distributed storage and decentralization. In the blockchain financial and economic application layer, there are tradable financial products, digital asset management, third-party payment and cross-border payment besides the more mature virtual currency, all of which are the mainstream scenarios based on distributed super-book accounts.

2.3 Specific application areas of blockchain finance and economics

Blockchain technology is used in different aspects of the financial and economic sector, this article summarizes the mainstream applications as follows:

2.3.1 Application 1: Cryptocurrency and its trading platforms

The birth of Bitcoin marked a new type of asset-Cryptocurrency, which was invented by an unknown person or group of people under the name Satoshi Nakamoto and released as open-source software in 2009 (Davis, 2011). Bitcoin is the first decentralized cryptocurrency and worldwide payment system without a central bank or single administrator. The network is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a blockchain (Tschorsch & Scheuermann, 2016). There are many other types of cryptocurrency in addition to the bitcoin, such as Ethereum (which is an open source software platform based on blockchain technology that is not only a cryptographic currency but also can be used by programmers to pay for transaction costs and services in the Ethereum network), **Bitcoin Cash** (it generated after bitcoin's hard fork), **Ripple** (it's a global clearing house for other currencies or other value entities such as the U.S. dollar, the euro, the pound sterling, bitcoin and airline miles, commodities), **Litecoin** (is an early replacement of bitcoin designed to allow ordinary people to mine as well) and **Dash** (It has a unique, two-tiered network compared to bitcoin which can be paid in an instant). According to the statistics (Sina comprehensive, 2017), the total market value of cryptocurrencies is about 600 billion$ at present, bitcoins accounted for 323 billion$, followed by Ethereum (71 billion$), bitcoin cash (32 billion$), Ripple (29 billion$) and Litecoin (176 billion$). It's clear that cryptocurrency has attracted the attention of more and more countries and become an indispensable part of the application of blockchain finance and economics. A number of virtual currencies trading platforms have emerged in different countries around the world, this article classifies some active virtual currency platforms according to their companies' registration place: there are 8 platforms registered in Hong Kong (Binance, Bitfinex, Gate.io, ZB.com, EXX.com, Coinw.com, OKEX, Coincola); 2 in UK (COINEGG , Hitbtc); 2 in Singapore (Huobi.pro, CEX.COM); 2 in Japan (Bitflyer, Coincheck); 1 in Korea (Bithumb); 1 in Seychelles (Bitmex); 1 in USA (KuCoin); 1 in Taiwan (OTCBTC) and 1 in Finland (Localbitcoins). These platforms support the exchange between multiple currencies and exchange between legal and virtual currencies, the trading of virtual currency has been going on for years all over the world.

2.3.2 Application 2: Cross-border payment

Cross-border payments generally refer to the transnational and trans-regional transfer of funds between two or more countries or territories through international trade, international investment and other international claims and debts with certain settlement instruments and payment systems. The traditional cross-border payment is based on the banking system which has the characteristics of time-consuming, high cost, more funds occupied and low security, but all these bottlenecks can be effectively overcome when we apply blockchain in cross-border payment to reconstruct the credit system and expand the payment boundary. One author (Ba, 2016) pointed out that the application of blockchain technology in the field of cross-border payment has a very high potential effect and its development is divided into three stages. The panel (Holotiuk, Pisani, & Moormann, 2017) believe that blockchain technology will improve the payment system by providing a solid structure for cross-border transactions and removing expensive intermediary costs and gradually weaken or alter the business model of existing payment industries. Yao & Zhu (2017) proposed a path of blockchain acting on cross-border payment based on the exploration of the application of VISA and SWIFT blockchain. Authors (Crosman, 2017) pointed out that R3 is working with 22 of its member banks to build a real-time, cross-border payments solution on Corda, the consortium's "blockchain inspired" distributed ledger. Nadeem (2017) indicated that the American Express FX International Payments business is working with Ripple, a provider of enterprise global blockchain solutions, to make blockchain payments commercially available. Sheila James, vice president of operations at business-to-business payment platform Veem, emphasized that their blockchain system is able to provide more real-time data for small business clients (Turner, 2017).

2.3.3 Application 3: Digital asset registries and management

Following digital currencies and money transfer, one of the biggest blockchain applications in development is digital asset registries and management. The blockchain technology can record, transfer, and verify asset ownership (home, auto, stocks, bonds, mortgages, and insurance), and also to preserve the integrity and authenticity of sensitive

documents or records (e.g., passports, visas, driver's licenses, birth and death certificates, voter registration, contracts, wills, patents, and medical records). An exemplary implementation of digital asset registries for identity services is the State of Illinois's blockchain-based birth registry project (Evernym.com,2017). Gail A. Van Norman & Roï Eisenkot (2017) showed us how to identify and register digital asset clearly, and identified that digital asset award exclusive rights to works of creative authorship, including works of fiction, nonfiction, music, choreography, and architecture. Some authors (Spencer & Belcher, 2017) said that Blockchain patenting activity in the U.S. includes applications filed by major financial institutions and large technology companies like Amazon.com and Blockchain focused startups like Coinbase, and some companies are filing for Blockchain-related patents to protect the digital asset.

3. The challenges of blockchain finance and economics

3.1 The limits of blockchain technology itself

Blockchain is an innovation in Internet finance technology, which involves in cryptology, computer science, artificial intelligence and other disciplines of integrated cutting-edge technology with high development costs and high difficulty of development. The blockchain is added to the bill every ten minutes and runs more slowly. Each block's capacity is only 1MB and the online transactions allow only 8 times per second business, which has a far gap with the current third-party payment named Alipay which supports thousands of transactions per second. Blockchain establishes credit guarantee of trusted intermediary through program algorithm, but its information is irreversible which brings the system more difficult to recover debt and once the private key password is lost or leaked, it will cause irreparable loss of customer assets. Although the technical logic of the blockchain is clear and theoretically difficult to be violently cracked, the possibility of tampering with the data still exists through the hostage of a large number of zombies or the operation mode of a trade union cluster. So technical risks such as hackers must be concerned with the expansion of the scope and amount of blockchain.

3.2 More difficulties in financial regulation

Financial regulation is a powerful guarantee for Internet financial information security, but the emergence of blockchain finance and economics bring a decentralized, network-less Internet system which greatly increased the relevance and effectiveness of financial regulation. At present, people have a relatively low understanding and acceptance of the blockchain and it is hard to identify real and effective blockchain financial products. It is difficult for regulators to lock in many anonymous accounts of clients and understand the whereabouts of funds, the absence of a central system has facilitated convenience for criminals' money laundering, fraud, and tax evasion but increased the difficulty of national supervision. Currently, in addition to bitcoin as the first cryptocurrency that is relatively hot at home and abroad, other applications of blockchain finance and economics such as P2P finance, third-party payment and other areas of Internet finance are in the exploration stage needed to be further developed and improved.

3.3 Complicated straits in global collaboration

The layout of blockchain finance and economics in the global smooth is very difficult due to the great cultural diversities and liberal democracy. The use of some kind of virtual currency as an equivalent in order to achieve real-time global liquidation is a challenge for the central bank's legal tender and the right of payment to some extent. The legal tender is endorsed by national credit, but the virtual currency credit is the mathematical algorithm that is difficult to reflect the financial will of any single country. We take bitcoin as an example, only a few countries such as Japan, Germany, and the United States recognize the legal status of bitcoin at present, most countries cannot accept its monetary attributes especially China. Therefore, the further application and development of blockchain technology in global financial and economic field need to weigh the interests of all countries to reach a consensus.

4. The countermeasures of blockchain finance and economics

4.1 Promoting the research and exploitation of financial and economic blockchain technology

The development of the blockchain application project in the financial and economic fields have been highly concerned by the international financial giants, research and development of related projects are

continuously promoted at present. However, the application of blockchain finance and economics in various countries is still in its infancy, there exists not only weak foundation of the related research but also quite complicated difficulties encountered in the implementation process. Therefore, all countries should set up the State Key Laboratory of Blockchain Finance lead by the Central Bank or other agencies according to their own country's research and development strength. R & D should be stepped up in cross-border payments, cross-bank settlement of banks, digital currency, securities issuance and data notes. Countries and governments should construct a number of general-purpose application service platform to provide the appropriate payment for financial enterprises aiming at finding a reliable solution by combining the unique features of the financial system and blockchain technology.

4.2 Accelerating the preparation and implementation of relevant standards

"Standard" is not only a passport for the development and application of blockchain in financial and economic industries but also the basic guarantee for the industry to be normative and ordered. The standard battle around the application of blockchain has started at the moment, the blockchain technology supplier named Chain has cooperated with the world's leading financial institutions such as Citigroup, Fidelity, First Data and MUFG and already announced the Chain Open Standard. This standard has made a big breakthrough in the financial blockchain consensus model, private data encryption, intelligent contract operation and scalable data model and has used by some leading financial companies. However, it’s a complex and arduous task to develop standards that are applicable in all countries to satisfy different culture and financial systems, so we need every country to work hard together step by step to promote blockchain finance and economics from shallow to deep.

4.3 Encouraging alliances and cooperation among different industries

There involve many different types of subjects from the blockchain technology research to the financial industry application level, which objectively increases the complexity and coordination difficulties of the technical cooperation in the blockchain. Financial market participants, technology companies, regulators and other entities need to strengthen communications and coordination to establish an effective, lasting and in-depth cooperation mechanism. The Central Bank should actively promote the linkage and cooperation between the upstream and downstream industries at home and abroad to realize autonomous control in technology application and ensure the safety of financial information. The leading companies and industries are responsible to form alliances to provide "wind vane" for the global blockchain finance and economics. The government, financial institutions, technical service providers, universities and research institutes are all important participants in the complicated systematic project of blockchain finance and economics, all possible problems and difficulties can be solved only when all participants work together to form strong synergies.

4.4 Strengthening the financial supervision of blockchain

Financial supervision is the use of power to ensure financial innovation develops orderly and provide escorts for blockchain finance and economics. Regulators need to consider the following four questions at least: (1) What should be the direction of regulatory reform? The divisional regulation or mixed regulation? (2) How to balance the privatization of proceeds and the cost of socialization? (3) How to protect the interests of depositors? (4) How to get the authorization of regulatory measures? So what should regulatory authorities do firstly is to develop relevant standards and regulations trying to apply the prevention means of blockchain technology to the detection of the Internet value delivery. For the purpose of improving the blockchain financial and economic service quality, they can consider using smart contracts to effectively track criminal activities. Secondly, as the new technology will have a profound impact on the monetary system in various countries, the regulation and control of monetary policy will not keep up with the situation changes, so the regulatory authorities should keep pace with the times and constantly improve the regulatory measures so as to strengthen the international supervision of blockchain finance and the international cooperation committed to establishing a unified global regulatory system to eliminate transnational crime. Lastly, the supervision of financial institutions engaging in financial derivatives should be strengthened, government authorities need to stipulate the minimum capital of financial institutions admitted to derivatives transactions and require disclosure of its accounting

standards and internal control risk measures on the purpose of establishing high-quality measures of information disclosure.

5 Conclusion

Blockchain technology is considered as a disruptive innovation following steam engines, electricity and the Internet. As we all known that steam engines and electricity have emancipated productivity, the internet has changed the way information is delivered, in that way the blockchain will likely change the way value is delivered as a machine for building trust. Blockchain technology has solved two major problems of the digital economy: One is that once the assets are digitized all their flow can be found through the chain; the other is that the zero-cost trust has been truly built under anonymous society, which bring new opportunities for the current Internet economy. Although the decentralized nature of blockchain technology has been a boon to many financial and economic industries, it has encountered many obstacles to its application and development. Therefore, blockchain technology is a double-edged sword for traditional economic and financial development, which places a higher demand on regulators' data-processing and risk-response capabilities, then what we need to do is to explore the application environment of blockchain finance and economics from the perspectives of technology, applicability, regulation, supervision and so on aiming at benefiting the whole society.

References

[1] Ba, J. (2016). The prospect of blockchain application in cross - border payment field. Retrieved from http://www.10tiao.com/html/328/201611/2650872474/1.html (February 1, 2018).

[2] Chen, F. (2017). A Probe into the Dialectical Relationship between Money and Freedom - From the Perspective of Marxist Economic Philosophy. *Nanjing Social Science*, (08), 75–81.

[3] Cowley, S. (2017). 2.5 Million More People Potentially Exposed in Equifax Breach. *The New York Times*. Retrieved from https://www.nytimes.com/2017/10/02/business/equifax-breach.html (January 16, 2018).

[4] Cristian, O., Tudor, O., & Bolos, M. (2010). Information Asymmetry Theory in Corporate Governance Systems. *Annals of the University of Oradea: Economic Science*, *1*(2), 516–522.

[5] Crosman, P. (2017). R3 to take on Ripple with cross-border payments blockchain. *American Banker; New York, N.Y.* Retrieved from https://search-proquest-com.ucd.idm.oclc.org/docview/1957965453/citation/F4C0367615-95447CPQ/1 (January 17, 2018).

[6] Davis, J. (2011). The Crypto-Currency. *The New Yorker*. Retrieved from https://www.newyorker.com/magazine-/2011/10/10/the-crypto-currency (January 10, 2018).

[7] Evernym.com. (2017). State of Illinois Partners with Evernym to Launch Birth Registration Pilot. Retrieved from http://globenewswire.com/news-release/2017/08/31/1106400/0/en/State-of-Illinois-Partners-with-Evernym-to-Launch-Birth-Registration-Pilot.html (December 23, 2017).

[8] Gail A. Van Norman, M. D., & Roï Eisenkot, Bs. (2017). Technology Transfer: From the Research Bench to Commercialization. *JACC: Basic to Translational Science*, *2*(2), 197–208.

[9] Holotiuk, F., Pisani, F., & Moormann, J. (2017). The Impact of Blockchain Technology on Business Models in the Payments Industry. *Wirtschaftsinformatik 2017 Proceedings*. Retrieved from https://aisel.aisnet.org/wi2017-/track09/paper/6 (December 29, 2017).

[10] Illing, G., & Peitz, M. (2005). Understanding the Digital Economy: Facts and Theory Introduction. *CESifo Economic Studies; Oxford*, *51*(2/3), 187–188.

[11] Khandelwal, S. (n.d.). It's 3 Billion! Yes, Every Single Yahoo Account Was Hacked In 2013 Data Breach. Retrieved from http://thehackernews.com/2017/10/yahoo-email-hacked.html (January 7, 2018).

[12] Nadeem, K. (2017). American Express introduces blockchain-enabled cross-border payments. *SNL European Financials Daily; Charlottesville*. Retrieved from https://search-proquest-com.ucd.idm.oclc.org/docview/1966280977/abstract/-66E26FBCFED74C26PQ/1 (January 10, 2018).

[13] Sina comprehensive. (2017). Next bitcoin? This digital currency rose 7000% this year. Retrieved from http://finance.sina.com.cn/money/forex/bitcoin/2017-12-20/doc-ifyptfcn2507913.shtml (February 1, 2018).

[14] Spencer, L., & Belcher, M. (2017). Defensive Patenting Strategies For Blockchain Innovators. *ROPES&GRAY*. Retrieved from http://www.ropesgray.com/newsroom/alerts/2017/10/Defensive-Patenting-Strategies-For-Blockchain Innovators.-aspx (February 2, 2018).

[15] Swan, M. (2015). Blockchain: Blueprint for a New Economy. Retrieved from https://www.goodreads.com/-work/best_book/44338116-blockchain-blueprint-for-a-new-economy (November 15, 2017).

[16] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys Tutorials*, *18*(3), 2084–2123. https://doi.org/10.1109/COMST.2016.2535718.

[17] Turner, E. (2017). Blockchain cross-border payments face hurdles before realizing benefits. *SNL Financial Extra; New York*. Retrieved from https://search-proquest-com.ucd.idm.oclc.org/docview/1902321368/abstract/FF8EF05AEF9C-421DPQ/1.

[18] Yao, X., & Zhu, T. (2017). Blockchain is to create a new ecology of cross-border payment. *Financial Expo (wealth)*, (05), 46–48.

[19] Zhou, J., Li, W., & Guo, G. (2017). Patent pattern analysis of Blockchain technology. *Telecommunication Network Technology*, (03), 37–42.